

**FILED**

## UNITED STATES DISTRICT COURT

SOUTHERN

DISTRICT OF

ILLINOIS SEP 26 2018

CLERK, U.S. DISTRICT COURT  
SOUTHERN DISTRICT OF ILLINOIS  
EAST ST. LOUIS OFFICE

## In the Matter of the Search of

(Name, address or brief description of person, property or premises to be searched)

Information associated with e-mail accounts  
joshua.breckel@yahoo.com, joshuabreckel@yahoo.com,  
and epicdude22@yahoo.com, that is stored at premises  
controlled by Oath Holdings, Inc., 701 First Avenue,  
Sunnyvale, California 94089

**APPLICATION AND AFFIDAVIT  
FOR SEARCH WARRANT**

Case Number:

3:18-mj-3201-DGW

I, Tyrone Forte being duly sworn depose and say:I am a(n) Special Agent with the Federal Bureau of Investigation and have reason to believe  
Official Titlethat ☐ on the person of or ☒ on the property or premises known as (name, description and/or location)

See Attachment A

in the Northern District of California

there is now concealed a certain person or property, namely (describe the person or property to be seized)

See Attachment B

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

evidence, fruits, and instrumentalities

concerning a violation of Title 18 United States code, Section(s) 875(d), 2251(a), 2252A(a)

The facts to support a finding of probable cause are as follows:

See attached affidavit.

Continued on the attached sheet and made a part hereof:

☒ Yes ☐ No

Signature of Affiant

Sworn to before me and subscribed in my presence,

September 26, 2018

Date

at

East St. Louis

Illinois

City

State

Donald G. Wilkerson

US Magistrate Judge

Name of Judge

Title of Judge

Signature of Judge

FILED

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF ILLINOIS

SEP 26 2018

CLERK, U.S. DISTRICT COURT  
SOUTHERN DISTRICT OF ILLINOIS  
EAST ST. LOUIS OFFICE

IN THE MATTER OF THE SEARCH OF  
Information associated with e-mail accounts  
**joshua.breckel@yahoo.com**,  
**joshuabreckel@yahoo.com**, and  
**epicdude22@yahoo.com**, that is stored at  
premises controlled by Oath Holdings, Inc., 701  
First Avenue, Sunnyvale, California 94089

Case No. 3:18-mj-3201-DGW

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Tyrone Forte, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) assigned to the FBI's Springfield Division, Fairview Heights Resident Agency, in Fairview Heights, Illinois. I have been so assigned for approximately twenty-seven (27) years. During the last seventeen (17) years, I have primarily investigated matters involving Violent Crimes Against Children, to include the sexual exploitation and abuse of children, particularly regarding the illegal trafficking and transportation of minors for illegal sex acts and prostitution, and the production, distribution, receipt, and possession of child pornography involving the internet. During my career as a Special Agent, I have investigated and assisted in the investigations of a variety of federal violations, including wire fraud, mail fraud, Medicare and health insurance fraud, corruption of state and local public officials, violent crimes, illegal drug conspiracy and drug distribution rings, computer and internet related crimes involving intrusions, frauds and identity theft. From 2005 until 2015, I served as an FBI certified computer forensic examiner. I have worked on or assisted in over 250 cases involving sex trafficking, child pornography trading, distribution, and manufacturing. I have been trained in the search, discovery, and recovery of electronic evidence from computers, cell phones, computer peripherals, and computer data, by imaging computer hard drives and interpreting on-line computer activity from computers, data logs and Internet Service Providers.

2. I make this affidavit in support of an application for a search warrant for information associated with e-mail accounts **joshua.breckel@yahoo.com**, **joshuabreckel@yahoo.com**, and **epicdude22@yahoo.com** that is stored at premises owned, maintained, controlled, and operated by Oath Holdings, Inc., an e-mail provider headquartered at 701 First Avenue, Sunnyvale, California 94089. The information to be searched for and seized is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Oath Holdings, Inc. (also known as "Yahoo") to disclose to the government records and other information in its possession, including the contents of communications, pertaining to an ongoing investigation.

3. More specifically, I am seeking a search warrant for the contents of e-mail accounts **joshua.breckel@yahoo.com**, **joshuabreckel@yahoo.com**, and **epicdude22@yahoo.com** that have been used in connection with the Production, Distribution, Receipt, and/or Possession of Child Pornography in violation of 18 U.S.C. §§ 2251(a) and 2252A(a).

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

#### STATUTORY AUTHORITY

5. Title 18, United States Code, Section 2703(a) provides that, pursuant to a search warrant issued by a court of competent jurisdiction, a governmental entity may require a provider of electronic communication service to disclose the contents of an electronic communication that has been stored electronically for 180 days or less.

6. Title 18, United States Code, Section 2703(b)(1)(A) provides that, pursuant to a search warrant issued by a court of competent jurisdiction, a governmental entity may require a provider of remote computing service to disclose the contents of an electronic communication that has been stored electronically for more than 180 days.

7. Title 18, United States Code, Section 2703(c)(1)(A) provides that, pursuant to a search warrant issued by a court of competent jurisdiction, a governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications).

8. Title 18, United States Code, Section 2711 defines “remote computing service” as “the provision to the public of computer storage or processing services by means of an electronic communications system.”

9. Title 18, United States Code, Section 2711 defines “governmental entity” to include any department or agency of the United States and defines “court of competent jurisdiction” to include any district court of the United States (including a magistrate judge of such a court) that has jurisdiction over the offense being investigated.

#### TECHNICAL BACKGROUND

10. In my training and experience, I have learned that Oath Holdings, Inc. provides a variety of on-line services, including electronic mail (“e-mail”) access, to the general public. Subscribers obtain an account by registering with Oath Holdings, Inc (also known as “Yahoo”). During the registration process, Yahoo asks subscribers to provide basic personal information. Therefore, the computers of Oath Holdings, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Yahoo subscribers) and information concerning subscribers and their use of Yahoo services, such as account access information, e-mail transaction information, and account application information.



11. In general, an e-mail that is sent to a Yahoo subscriber is stored in the subscriber's "mail box" on Yahoo servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Yahoo servers indefinitely.

12. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Yahoo's servers, and then transmitted to its end destination. Yahoo often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Yahoo server, the e-mail can remain on the system indefinitely.

13. A Yahoo subscriber can also store files, including e-mails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by Oath Holdings, Inc. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mails in the account, and attachments to e-mails, including pictures and files.

14. Subscribers to Yahoo might not store on their home computers copies of the e-mails stored in their Yahoo account. This is particularly true when they access their account through a public terminal, or if they do not wish to maintain particular e-mails or files in their residence.

15. In general, e-mail providers like Yahoo ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

16. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Yahoo's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers, smart phones, or other devices were used to access the e-mail account.

#### PROBABLE CAUSE

17. On about April 9, 2018, the Middlesex Borough, New Jersey Police Department (MBPD) received a complaint from the family of C.S., a white juvenile female, DOB August 20, 2002, residing in Middlesex, New Jersey 08846. C.S. reported being extorted via internet application Whisper by username "User\_Pure" and Snapchat username "thatonekiduknol" for explicit/nude photographs. The individual offered to donate \$2,500 to C.S.'s high school GoFundMe account in exchange for nude pictures. A screen capture of the individual's bank account was sent to C.S. and it showed that he had the money to make the donation.

18. During their conversations over Snapchat, C.S. eventually sent the individual a nude picture of her face and breasts, while holding up three fingers as he requested. The individual

began offering \$5,000 if C.S. had other friends who could also send photographs or make a video with her.

19. Local investigation by the MBPD included a search of the victim's mobile phone and the issuance of New Jersey state court subpoenas to Snapchat and Whisper. The Snapchat account "thatonekiduknol" was created September 21, 2015 with the associated e-mail address of hdheh@heje.com and the associated mobile telephone number of 618-960-7572. A recently associated IP Address was 97.86.204.188. Whisper records indicate the "User\_Pure" account also had recent IP Address logins from 97.86.204.188.

20. A subpoena response from Sprint revealed that the associated subscriber of phone number 618-960-7572 was Victoria Breckel, 1210 Larkspur Drive, Mascoutah, Illinois 62258 with another associated number of 618-566-2940. Investigation by Detective Jared Lambert of Mascoutah, Illinois Police Department (MPD) on May 21, 2018 also revealed that Victoria Breckel's son JOSHUA P. BRECKEL primarily utilized the mobile telephone 618-960-7572.

21. On May 21, 2018, Det. Lambert responded to Victoria Breckel's residence in Mascoutah and made contact with JOSHUA BRECKEL. BRECKEL agreed to come to the Mascoutah Police Department to make a voluntary statement. At the MPD, BRECKEL was Mirandized and participated in a video-recorded interview. Det. Lambert also seized BRECKEL's iPhone as he had probable cause to believe it contained evidence relevant to the investigation of the Attempted Production of Child Pornography and Extortion.

22. BRECKEL stated that he was an almost 20-year old college student who resided full-time with his mother Victoria at the Mascoutah address. BRECKEL identified his online accounts as e-mail address: joshua.breckel1@gmail.com; and Facebook profile "Joshua Breckel." BRECKEL confirmed his mobile telephone number was 618-960-7572 and was the phone number associated with the iPhone seized by Det. Lambert.

23. Over the course of his interview, BRECKEL admitted to using Snapchat to obtain a topless photograph of C.S. whom BRECKEL stated he believed to be a 14-year old female. BRECKEL further admitted to threatening C.S. by telling her that he would publicly share the nude photograph she had already sent him if she did not send more nude images and videos.

24. BRECKEL further admitted to Det. Lambert that both his iPhone (618-960-7572 phone number) and his laptop computer would contain images of child pornography. BRECKEL signed a written consent to search form for his iPhone.

25. In BRECKEL's presence, Det. Lambert went through BRECKEL's iPhone images, seeing several images of minor females that he believed to be child pornography. Det. Lambert asked BRECKEL about each image and in each instance, BRECKEL identified an age for the minor depicted in the photograph. The ages ranged between 11 and 16 years old. Det. Lambert also discovered a screen shot of a Snapchat message thread where it appears that BRECKEL was extorting a minor female for nude images.

26. Det. Lambert and another MPD officer escorted BRECKEL back to his mother's residence. At the residence, BRECKEL led Det. Lambert to a laptop computer and external storage device. Both were seized. They then returned to the MPD. BRECKEL was again

Mirandized and the video-recorded interview continued. BRECKEL signed written consent to search forms for his computer and storage device.

27. On May 22, 2018, Det. Lambert and I conducted a preliminary forensic review of the phone, computer and external storage device. Our review discovered multiple images and videos of child pornography and evidence that BRECKEL had been using multiple social media applications to obtain child pornography images and videos from victims via extortion, purchase, or trade.

28. In June 2018, I sent court orders per 18 U.S.C. § 2703(d) to the social messaging applications Kik, MeetMe, Whisper and Snapchat for accounts linked to BRECKEL. An initial review of the returned materials indicates that BRECKEL would use these applications to obtain child pornography images and videos from victims via romance, purchase, extortion and trade. BRECKEL would also trade the images he received with other users in Kik chat rooms in exchange for additional images and videos of child pornography.

29. On July 6, 2018, BRECKEL was charged by complaint in federal district court in the Southern District of Illinois with one count of Receipt of Child Pornography (18 U.S.C. § 2252A(a)(2)(A)) and one count of Interstate Communications With Intent to Extort (18 U.S.C. § 875(d)). On July 18, 2018, a grand jury indicted BRECKEL on these same two charges. He has been in custody continuously since he was charged by complaint.

#### Proffer Statements

30. On July 31, 2018, and August 24, 2018, I conducted proffer interviews with BRECKEL in the presence of BRECKEL's attorney and AUSA Christopher Hoell. During the course of these two interviews, BRECKEL admitted to using a wide variety of social media applications, e-mail accounts, and other platforms both mobile and desktop to produce, receive, distribute, and transport child pornography.

31. By his own estimation, BRECKEL obtained nude images and videos from approximately 100 female victims. BRECKEL obtained these images through feigning romantic interest, extortion, trade and purchase. BRECKEL stated that while some of the victims were adults, the majority were minors. BRECKEL further stated that he extorted some of his adult victims as well as his minor victims by threatening to reveal nude images to their friends, family, and social media contacts if the victims did not provide specific nude images and videos he demanded.

32. BRECKEL provided that the Yahoo e-mail accounts **joshua.breckel@yahoo.com**, **joshuabreckel@yahoo.com**, and **epiedude22@yahoo.com** were used to extort women and girls over the internet, to directly distribute or receive child pornography, and/or to sign up for the various social media applications he used to obtain extorted images or child pornography from victims. BRECKEL further advised that child pornography would be found in these e-mail accounts' saved and sent e-mail messages.

#### INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

33. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to

require Yahoo to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

34. Based upon the above, there is probable cause that BRECKEL has used the **joshua.breckel@yahoo.com**, **joshuabreckel@yahoo.com**, and **epicdude22@yahoo.com** e-mail accounts for interstate extortion, in violation of 18 U.S.C. §875(d), and to produce, distribute, receive, transport, and possess child pornography in violation of 18 U.S.C. §§ 2251 and 2252A(a).

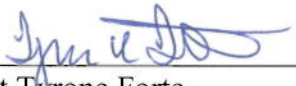
35. Therefore, based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in the control of Oath Holdings, Inc. there exists evidence of a crime and contraband or fruits of a crime. Accordingly, a search warrant is requested.

36. I respectfully request that the Court issue a search warrant directing Oath Holdings, Inc. to disclose any and all information described in Attachment B, to the extent that such information is in its care, custody and control.

37. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. See 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offenses being investigated. 18 U.S.C. § 2711(3)(A)(i).


38. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

I certify that all of the information set forth above is true and correct to the best of my knowledge and belief.

  
\_\_\_\_\_  
Special Agent Tyrone Forte  
Federal Bureau of Investigation

Subscribed and sworn to before me  
on this the 26 day of September, 2018.

  
\_\_\_\_\_  
DONALD G. WILKERSON  
UNITED STATES MAGISTRATE JUDGE

  
\_\_\_\_\_  
Christopher R. Hoell  
Assistant United States Attorney

**ATTACHMENT A**

Place to Be Searched

This warrant applies to information associated with the Yahoo e-mail accounts **joshua.breckel@yahoo.com**, **joshuabreckel@yahoo.com**, and **cpicdudc22@yahoo.com** that is stored at premises owned, maintained, controlled, or operated by Oath Holdings, Inc., a company headquartered at 701 First Avenue, Sunnyvale, California 94089.



**ATTACHMENT B**

Particular Things to be Seized

**I. Information to be disclosed by Oath Holdings, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Oath Holdings, Inc., Oath Holdings, Inc. is required to disclose the following information to the government for each e-mail account listed in Attachment A:

- (a) The contents of all e-mails stored in the account, including copies of e-mails sent from the account.
- (b) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number).
- (c) All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, videos, and other files.
- (d) All records pertaining to communications between Oath Holdings, Inc. and any person regarding the account, including contacts with support services and records of actions taken.
- (e) A list of all Oath Holdings, Inc. services to which the holder of the account has subscribed.
- (f) A list of any and all associated accounts.

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of the statutes listed on the warrant involving Joshua Breckel, including:

- (a) Records relating to interstate extortion and the production, distribution, receipt and possession of child pornography.
- (b) Records relating to who created, used, or communicated with the accounts listed in Attachment A.